CLAIMS

What is claimed is:

1. A method of processing a digital signal comprising the steps of:

a) receiving an encrypted signal at a first logical circuit;

b) determining a broadcast encryption key for said encrypted signal at a first location separate from said first logical circuit;

c) encrypting said broadcast encryption key;

d) transferring said encrypted broadcast encryption key over a communication link;

e) at said first logical circuit, decrypting said encrypted broadcast encryption key to determine said broadcast encryption key; and

f) at said first logical circuit, decrypting said encrypted signal using said broadcast encryption key.

2. The method of Claim 1 wherein said step c) comprises the steps of:

c1) accessing a value in a hidden register on said first logical circuit; and

c2) using said value accessed in said step c1), encrypting said broadcast encryption key.

3. The method of Claim 2 wherein said step c) further comprises the step of:

c3) modifying the value in said hidden register.

4. The method of Claim 1 further comprising the steps of:

g) storing a value in a hidden register on said first logical circuit; and

h) providing said value to a host computer system to use for encryption.

5. The method of Claim 1 wherein said step e) further comprises the steps of:

e1) accessing a value in a hidden register on said first logical circuit; and

e2) using said value accessed in said step e1), decrypting said encrypted broadcast encryption key.

6. The method of Claim 1 wherein said received bitstream is substantially compliant the with Motion Pictures Experts Group (MPEG) format.

7. The method of Claim 1 wherein said step c) further comprises the steps of:

c1) selecting at least one of a plurality of hidden registers on said first logical circuit to be used to encrypt said broadcast encryption key; and

c2) indicating said selection to said first logical circuit.

8. The method of Claim 1 wherein said step c) comprises the steps of:

c1) accessing a value in non-volatile memory on said first logical circuit; and

c2) using said value accessed in said step c1), encrypting said broadcast encryption key.

9. The method of Claim 8 wherein said non-volatile memory contains user-dependent data.

10. A method of processing a digital signal comprising the steps of:

a) generating a local encryption key;

b) transferring said local encryption key across a communication link to a first logical circuit and to a second logical circuit;

c) with said local encryption key, encrypting said digital signal at said first logical circuit;

d) transferring said digital signal to said second logical circuit; and

e) using said local encryption key, decrypting said digital signal at said second logical circuit, wherein said digital signal is transferred from said first logical circuit to said second logical circuit in an encrypted form.

11. The method of Claim 10 further comprising the step of:

f) before transferring said local encryption key across said communication link, encrypting said local encryption key.

12. The method of Claim 11 wherein said step f) comprises the steps of:

f1) accessing a value in a register in said first logical circuit; and

f2) based upon said value accessed in said step f1), encrypting said local encryption key.

13. The method of Claim 11 wherein said step f) comprises the steps of:

f1) accessing a value stored in a register in said second circuit; and

f2) based upon said value accessed in said step f1), encrypting said local encryption key.

14. The method of Claim 10 further comprising the step of:

f) issuing a command to said first logical circuit to modify a header in said bitstream to indicate that said bitstream is encrypted.

15. The method of Claim 14 wherein the command further indicates the type of encryption wherein said type is between even and odd.

16. The method of Claim 10 further comprising the step of:

f) switching said local encryption key between odd and even encryption.

17. The method of Claim 10 further comprising the steps of:

f) polling a first hidden register in said first logical circuit;

g) determining whether the value in said hidden register has been modified; and

h) stopping said processing of said digital signal if said register has been modified.

18. The method of Claim 17 further comprising the step of:

i) sending a message to a broadcast provider if said step j) determined that said hidden register was modified.

19. A system for processing a digital signal, comprising:

a first logical circuit comprising a first hidden register and a local encryptor, said first logical circuit operable to decrypt a first local key using a first value stored in said first register; and

a second logical circuit comprising a local decryptor and a second hidden register, said second logical circuit operable to decrypt a second local key using a second value stored in said second register, said local decryptor operable to decrypt a signal encrypted with said local encryptor.

20. The system of Claim 19 further comprising:

a host processor;

a communication link connecting said host processor to said first logical circuit and to said second logical circuit; and

memory coupled to said host processor, said memory containing instructions which when run on said host processor are operable generate said first local key and to generate said second local key.

21. The system of Claim 20 wherein said memory further comprises instructions operable to access said first hidden register.

22. The system of Claim 19 wherein said first logical circuit further comprises:

a 1394 encryptor operable to encrypt a signal for transfer over an IEEE 1394 communication link.

23. The system of Claim 19 wherein said first logical circuit further comprises:

a broadcast decryptor comprising a broadcast hidden register, said broadcast decryptor operable to decrypt a broadcast signal and to decrypt an encrypted key using a value in said broadcast hidden register.

24. The system of Claim 22 wherein said memory further contains instructions which when run on said host processor are operable to generate a broadcast encryption key, to access said broadcast hidden register, and to encrypt said broadcast encryption key.

25. The system of Claim 19 wherein said first logical circuit further comprises a plurality of hidden registers and a control register operable to store a value to indicate which of said hidden registers is used for encryption.